INFORME DE CONCLUSIONES DEL EVENTO DE AEPD-ENISA SOBRE ESPACIOS DE DATOS

ESPACIOS DE DATOS EN LA UE: Sinergias entre protección de datos y espacios de datos, retos de la UE y experiencias españolas

I. INTRODUCCIÓN

Este informe tiene como objetivo presentar un extracto de los temas tratados en el evento: "*ESPACIOS DE DATOS EN LA UE: Sinergias entre la protección de datos y los espacios de datos, retos de la UE y experiencias españolas*". El evento fue organizado conjuntamente por la Agencia Española de Protección de Datos (AEPD) y la Agencia Europea de Ciberseguridad (ENISA) y las conclusiones correspondientes se derivaron principalmente de las sesiones de debate específicas organizadas durante la conferencia. Este evento se organizó y concibió como un mecanismo para hacer un análisis de la nueva regulación de la UE en los ámbitos digital y de datos y su interacción con la protección de datos. Entendemos esta conferencia como un ejercicio útil que permite una mejor aplicación del nuevo reglamento basado en el caso concreto de un Estado miembro de la UE.

Desde el anuncio anticipado del evento, la respuesta de numerosas partes interesadas fue positiva, reconociendo la necesidad de facilitar debates específicos sobre la aplicación de la normativa de la UE sobre espacios de datos. La comunidad interesados que asistieron a este evento representó una variada tipología de sectores y temas, y las discusiones y conclusiones así lo reflejan. Sin embargo, debido a la complejidad del nuevo ecosistema de acceso a los datos, el trabajo que se avecina requerirá un mayor esfuerzo dirigido a niveles de compromiso más ambiciosos e inclusivos. En cualquier caso, este evento permitió demostrar el valor añadido de las interacciones multidisciplinares.

La regulación de los espacios de datos abarcará una parte sustancial de las tecnologías. Como complemento, el RGPD destaca la necesidad de un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una aplicación estricta. En este sentido, el RGPD no debe ser considerado como un requisito mínimo o formal de cumplimiento, sino como un mecanismo para proteger los derechos fundamentales de una manera efectiva que permita el control por parte de los ciudadanos de sus propios datos y generar confianza en un mercado interior dinámico que afecte a todos los sectores económicos.

Es evidente que cada una de estas tecnologías será abordada en espacios de datos. Es decir, podríamos decir que los espacios de datos son un hub común donde convergerán todas las tecnologías y sobre el que serán posibles nuevos beneficios para nuestra sociedad, siempre que exista un entorno de confianza adecuado. Sin embargo, es difícil tener un conocimiento profundo de las implicaciones derivadas del uso de tecnologías emergentes. Nuestra responsabilidad como miembros de los espacios de datos es

conocer los impactos o amenazas que podrían suponer para nuestro Estado de Derecho en general y para los derechos y libertades de cada persona o grupo de personas en particular. En este sentido, las Autoridades de Control son conscientes de la necesidad de dotarse de expertos que identifiquen las amenazas existentes en cada tecnología a la vez que proponen soluciones prácticas y consejos para garantizar los derechos y libertades de las personas físicas.

El desarrollo de los espacios de datos debe ir asociado, entre otros, a los nuevos avances en materia de privacidad (por ejemplo, las estrategias de cómputo a datos, el tratamiento federado, la privacidad diferencial o la generación de datos sintéticos, etc.). Hoy en día, existen muchas iniciativas y nuevas líneas de trabajo que pueden tener sinergias con los espacios de datos. Las acciones relacionadas con los espacios de datos deben involucrar a todos los sectores, incluidos el de investigación, el industrial y el académico. Sin embargo, es importante tener en cuenta que cuando se trata de derechos y libertades de las personas físicas y sus datos relacionados, se debe garantizar la protección de los datos personales.

En la Unión Europea hay que hacer hincapié en la importancia de dotar de confianza a los espacios de datos: confianza que se puede conseguir entendiendo la normativa de protección de datos como una herramienta de trabajo para garantizar la confianza desde el diseño con la necesaria transparencia y respeto a los valores éticos y sociales de nuestro Estado de Derecho.

Hay muchos desafíos orientados a los datos por delante que deberán abordarse en el contexto de los espacios de datos y la regulación relacionada. Sin embargo, las oportunidades son infinitamente mayores de lo que representan los problemas y la interacción multidisciplinaria y el valor agregado para la implementación. Si algo debe caracterizar a los espacios de datos, debe ser la colaboración entre el ecosistema de las partes interesadas de un espacio de datos específico donde se puedan conjugar diferentes puntos de vista en torno a un objetivo común. Con este entusiasmo, tanto la AEPD como ENISA quisieron organizar este evento, con el objetivo de aportar consideraciones útiles para el camino a seguir.

II. PANELES PRINCIPALES

En este apartado se recogen las principales ideas que cada uno de los participantes en los paneles del evento han querido transmitir a través de su participación.

A. ¿POR QUÉ HABLAMOS DE RGPD EN LOS ESPACIOS DE DATOS?

Este primer panel contó con dos oradores en representación de dos autoridades supervisoras, en sus roles similares como jefes de la unidad. Son los encargados de analizar el impacto de la tecnología y la innovación en la protección de datos en cada una de estas instituciones, quienes destacan la importancia de la protección de datos en estos escenarios de acceso masivo a datos.

1. Luis de Salvador Carrasco, AEPD

Como activo, los datos tienen la misma importancia que cualquier otro activo de la entidad. Es de esperar que una empresa, en lo que respecta a sus activos de datos, esté dispuesta a unirse a iniciativas de compartición de acceso a datos que mantengan bajo control sus conocimientos técnicos, su cuota de mercado, su propiedad intelectual, sus secretos empresariales, su competitividad y sus principios éticos y de cumplimiento. Ese control le dará a la empresa la confianza suficiente para ser un actor en el mercado de compartición de acceso a datos.

Ese control, y la confianza que las partes interesadas necesitan en la economía del acceso compartido a los datos, se denomina "soberanía del dato". La soberanía de los datos de las empresas, los investigadores, los Estados (que gestionan los activos/datos que pertenecen a los ciudadanos) y las personas físicas es el camino para "crear la confianza que permitirá que la economía digital se desarrolle en todo el mercado interior".

La forma de conseguir una "soberanía de datos" efectiva significa implementar una infraestructura abierta y federada, basada en la gobernanza, las políticas, las reglas y los estándares, que permita generar confianza en todos los grupos de interés mediante un control efectivo de sus activos de datos mediante herramientas de gestión, legales y técnicas. A esto se le llama espacio de datos. Los Espacios de Datos deben permitir el acceso a los datos, considerando que el acceso significa "el uso de los datos, de acuerdo con requisitos técnicos, legales u organizativos específicos, sin que ello implique necesariamente la transmisión o descarga de datos" (artículo 2.13 DGA). El acceso a los datos no significa la difusión de datos y, por supuesto, no significa la fuga incontrolada de datos. El acceso a datos significa implementar formas de extraer información, útil para un contexto previsto, de diferentes fuentes de datos con el propósito de crear valor.

La gestión y el uso de las tecnologías de mejora de la privacidad (Privacy Enhancing Technologies, o PETs, por sus siglas en inglés) pueden cumplir fines adicionales más allá de la protección de datos. Los PETs también pueden cumplir varios requisitos de gobernanza en un espacio de datos y funcionar como herramientas de "doble uso": requisitos del RGPD y otros requisitos que se derivan de las preocupaciones de las empresas, los organismos públicos, la sostenibilidad del mercado de la UE, la investigación de la UE y la seguridad del Estado. La integración de las herramientas de privacidad y los PETs en el modelo de gobernanza debe hacerse mediante el diseño de los Espacios de Datos. De esta manera, pueden funcionar como herramientas de "doble uso" que facilitan la implementación de la soberanía de datos y la confianza de la parte interesada para unirse a la compartición de acceso a datos. Por lo tanto, los DPO con un profundo conocimiento sobre la gestión de datos y las herramientas de privacidad desde el diseño deben participar en el diseño de los Espacios de Datos para ponerse al día con lo establecido en el RGPD: control de los propios datos,

confianza en la economía basada en datos, seguridad jurídica para todas las partes interesadas.

2. Luis Velasco, EDPS

El RGPD se erige como la piedra angular en la configuración del futuro de Europa basado en los datos, no como un impedimento, sino como una piedra angular en los florecientes espacios de datos europeos. Las partes interesadas en la economía de los datos deben encontrar formas de fusionar el crecimiento económico con la protección de los derechos fundamentales. Dado que la economía de los datos está a punto de convertirse en una parte vital del PIB de la UE y en un empleador importante, el RGPD actúa como una fuerza de equilibrio, garantizando que la búsqueda del potencial económico no eclipse la necesidad de defender los derechos individuales.

Existe un reconocimiento generalizado entre las partes interesadas, que van desde los responsables políticos hasta los líderes de la industria y los ciudadanos, de que los "ámbitos de datos seguros" facilitados por el RGPD son fundamentales. Estos ámbitos, o "espacios de datos", son necesarios para la economía de los datos. Permiten el flujo fluido de datos y, al mismo tiempo, preservan la privacidad y otros derechos fundamentales, sentando un precedente para la confianza y la seguridad en la era digital.

El Comité Europeo de Protección de Datos (EDPB) y el Supervisor Europeo de Protección de Datos (EDPS) han sido proactivos a la hora de evaluar las propuestas legislativas de la Comisión para configurar la economía de los datos. Su enfoque sigue siendo proteger los principios básicos del RGPD, evitando cualquier redefinición que pueda conducir a la ambigüedad legal y las complejidades que podrían surgir de la creación de nuevos marcos regulatorios. En particular, hacen hincapié en la importancia de la claridad y los más estrictos controles en ámbitos sensibles, como el uso secundario de los datos sanitarios, para evitar infracciones de los derechos individuales y garantizar la alineación con las normas del RGPD.

B. INICIATIVAS DE ESPACIOS DE DATOS EUROPEOS

El segundo panel, dirigido por el Supervisor Europeo de Protección de Datos (EDPS), tuvo como objetivo debatir sobre los espacios de datos europeos y el papel de la protección de datos y los derechos fundamentales. El espacio de datos de salud se abordó de forma recurrente no solo porque ha sido el primer espacio regulado por la UE, sino también porque el ámbito sanitario constituye un espacio de datos en el que los datos tratados son especialmente sensibles, por ejemplo, recogidos como categorías especiales de datos en virtud del RGPD.

1. Xabier Lareo López de Vergara, EDPS

El Espacio Europeo de Datos Sanitarios (EEDS) es el pionero de los 10 espacios de datos previstos por la Comisión en su estrategia de datos. Además, también se ocupa de los datos que son sensibles y están etiquetados por el RGPD como categorías especiales de datos. Poner el foco en el EEDS fue una decisión fácil.

El panel proporcionó una visión del EEDS desde tres ángulos diferentes.

En primer lugar, Owe Langfeldt (DG SANTE de la Comisión Europea) nos explicó la propuesta legislativa, que actualmente está siendo debatida por el Parlamento Europeo, el Consejo y la Comisión. Owe explicó la estructura y las principales disposiciones de la propuesta de Reglamento EEDS. Una propuesta que tiene como objetivo mejorar el acceso y la compartición de datos de salud electrónicos para la prestación de servicios sanitarios y con fines de investigación e innovación y regulación.

A continuación, Jan Penfrat, de European Digital Rights (EDRi), expresó las preocupaciones de EDRi sobre la propuesta legislativa y destacó lo que consideran sus principales problemas: un control insuficiente por parte de los usuarios, una definición demasiado amplia de los datos de salud y unos fines permitidos poco claros para el tratamiento.

Por último, Carlos Parra Calderón (Instituto de Biomedicina de Sevilla) ofreció una visión general de IMPaCT y HelathyCloud, dos proyectos que exploran cómo construir una infraestructura de IT (Tecnología de la Información) para lograr un compartición eficaz y seguro de datos de salud en toda Europa.

2. Owe Langfeldt, DG SANTE – EC

Owe Langfeldt, como experto en temas de privacidad relacionados con la propuesta de la nueva regulación del Espacio Europeo de Datos Sanitarios, habla sobre los puntos clave de la normativa en materia de protección de datos personales, así como hace una visión general de otros espacios de datos europeos.

El Espacio Europeo de Datos Sanitarios está concebido para mejorar los resultados de salud de los pacientes y el ahorro de costes en el sistema sanitario para las Administraciones. Se espera que se publique a finales de la primavera de 2024.

Él ha encontrado dificultades para que los interesados accedan a sus datos y, también, dificultades similares para los profesionales de la salud. Por otro lado, la interoperabilidad entre los diferentes sistemas nacionales de salud sigue mejorando implementando paquetes legislativos para los sistemas de historiales clínicos electrónicas y la tecnología necesaria. Señala que hasta ahora hay 11 países activos para garantizar la interoperabilidad y la compartición de datos entre los Estados miembros.

Aborda la importancia de utilizar datos anonimizados o, al menos, seudonimizados para la investigación y el papel relevante del órgano administrativo que gestionará el

acceso a los datos para la investigación. También hace mención específica a las barreras de entrada al mercado debido a la falta de competencia de los proveedores de sistemas.

Por último, hace un repaso de los actuales y heterogéneos proyectos de Espacios Europeos de Datos, de diferentes sectores, haciendo hincapié en la importancia del Espacio Europeo de Datos Sanitarios en términos de privacidad debido al tipo de categorías de datos.

3. Carlos Parra Calderón, Instituto de Biomedicina de Sevilla

La ponencia "European Data Spaces Initiatives: working on Trustworthy Health Research Data Infrastructures for the Success of Data Spaces" presentó una visión general de los aspectos de seguridad y protección de datos para tener en cuenta en los espacios de datos para la investigación sanitaria y biomédica basada en la experiencia adquirida en dos iniciativas, una nacional y otra europea. Teniendo en cuenta la normativa vigente, las responsabilidades del tratamiento y los riesgos que conlleva, todo ello debe preverse en el diseño de las infraestructuras y teniendo en cuenta como aspecto crítico las profundas necesidades de confianza de los proveedores de datos sanitarios con estas infraestructuras.

La iniciativa nacional es el programa de Ciencia de Datos de la infraestructura de investigación en Medicina de Precisión asociada a la Ciencia y la Tecnología "IMPaCT", impulsado por el Instituto Nacional de Salud Carlos III, que define un conjunto de recomendaciones para el manejo de datos sensibles en base al Esquema Nacional de Seguridad español. La iniciativa europea es la acción de coordinación y apoyo financiada por la Comisión Europea "HealthyCloud", que define una agenda estratégica para la Nube de Investigación e Innovación en Salud en Europa y define una serie de servicios para apoyar el marco legal y regulatorio aplicable.

4. Jan Penfrat, Derechos Digitales Europeos

Jan Penfrat, como representante de la sociedad civil, habla de los espacios de datos como un cambio fundamental con respecto a los principios del RGPD y, en particular, del espacio de datos sanitarios, ya que se trata de datos personales muy sensibles. Prefiere hablar de cómo compatibilizar el RGPD y los espacios de datos, en lugar de hablar de sinergias.

No está de acuerdo con la afirmación de que los datos son el nuevo petróleo, al menos en la forma en que se ha presentado, aunque sí está de acuerdo en que los datos personales son tan tóxicos como puede ser el petróleo, por lo que tendremos que recopilar lo menos posible (minimización de datos y limitación de la finalidad). En este sentido, considera que se ha modificado la posición inicial de la Comisión Europea en su propuesta. Hablamos ahora de los datos como un activo para las empresas, del mercado de datos y de los activos estratégicos como consecuencia del mercado creado por la DMA, a pesar de que esta normativa establece que la transferencia de datos entre guardianes de acceso y no guardianes de acceso no debe contener datos personales.

Todos estos escenarios se basan en una gran cantidad de datos recopilados de forma voluntaria. Sin embargo, se ha detectado que una gran mayoría de los ciudadanos europeos no se sentirían cómodos con la compartición de sus datos médicos. Se supone que el EHDS le da más control al paciente. Sin embargo, el uso secundario puede, de alguna manera, hacer lo contrario y dar el control de sus datos a terceros que se definen a sí mismos como con un interés de investigación. Por un lado, como ciudadanos esperamos el secreto con médico, pero por otro lado, para un uso secundario está completamente fuera del control del interesado quién y durante cuánto tiempo se utilizan sus datos. La innovación no puede anular los derechos fundamentales.

> *La información personal no es una mercancía, es una representación de nuestro derecho a la privacidad y mercantilizarla nos trae una madriguera de conejo que creo que muy rápidamente dejará obsoleto nuestro derecho fundamental a la privacidad.*

Destaca como conclusión el manejo adecuado del consentimiento informado del paciente y la opción de exclusión.

C. INTERACCIÓN RGPD-DGA-DA-DMA-DSA-EHDS-AIA EN ESPACIOS DE DATOS

El tercer panel estuvo dirigido por el EDPB y abordó el impacto del nuevo Reglamento sobre el paquete digital en los espacios de datos y la protección de datos desde una perspectiva de la UE. Todas estas regulaciones tendrán una relación muy estrecha en estos escenarios de acceso a datos masivos, los espacios de datos. En este sentido, este panel contó con tres expertos europeos en protección de datos, con una sólida experiencia en el análisis de la regulación y la tecnología.

1. Anna Lytra, EDPB

Anna Lytra, del equipo de la oficina del delegado de protección de datos del EDPB, quiere abordar con este panel algunos aspectos de la nueva normativa del paquete digital europeo que tienen cabida en los espacios de datos. Para ello, cuenta con tres destacados ponentes en el ámbito de la privacidad aplicada a las tecnologías digitales.

2. Marit Hansen, Autoridad de Protección de Datos de Schleswig-Holstein

La intervención de Marit Hansen, reconocida por su trayectoria en privacidad y protección de datos con un perfil técnico, así como por su amplio conocimiento jurídico a lo largo de su extensa trayectoria profesional, se centra en señalar varios aspectos de alto nivel que tienen que ver con el nuevo paquete normativo digital y el RGPD.

> *Solo una frase: con los nuevos reglamentos europeos, el RGPD no se ve afectado.*

Los desarrollos y aplicaciones resultantes de la nueva normativa tendrán que adaptarse para cumplir con el RGPD, por lo que será necesario desarrollar soluciones viables.

Un aspecto primordial será abordar los términos de detección y mitigación de riesgos al analizar la interacción entre el RGPD y las nuevas leyes, en particular la Ley de IA, que

influirá en la forma de adaptar la tecnología y las organizaciones a los riesgos de los derechos y libertades de las personas físicas. A este respecto, debería llevarse a cabo una evaluación de impacto "profesionalizada "sobre los derechos fundamentales.

Por último, como observación final, dado que la mayoría de las nuevas leyes crean su propia autoridad de supervisión con su propia terminología jurídica, la coordinación entre ellas será una cuestión clave.

3. Regina Becker, Servicio Nacional de Datos de Luxemburgo

La creación de espacios de datos es uno de los principales objetivos de la Estrategia de Datos de la UE. Los actos legislativos recientes son la Ley de Gobernanza de Datos y dos proyectos de Reglamento, la Ley de Datos y el Espacio Europeo de Datos Sanitarios. Sin embargo, cuando se trata de crear espacios de datos para uso secundario, un espacio con datos armonizados disponibles en el marco de una gobernanza de datos armonizada, resulta evidente que estos Reglamentos no proporcionan una base jurídica para armonizar y conservar los datos para uso secundario.

No es fácil aplicar formas alternativas de crear espacios de datos armonizados para el uso secundario de datos personales sensibles. La mayoría de las entidades que han recopilado datos para sus fines primarios no tienen una base legal para armonizar los datos para uso secundario ni para compartirlos sistemáticamente para los fines de los usuarios. Su misión y, por tanto, su base jurídica se centra enteramente en sus propias tareas primarias. Incluso cuando las entidades tienen la misión de hacer que los datos estén disponibles para un uso secundario, cada entidad tiene su propia gobernanza de datos por ley, lo que conduce a una fragmentación en toda Europa. El consentimiento, con su exigencia de ser informado y específico, tampoco es adecuado para la divulgación a los usuarios.

Los espacios de datos armonizados para los datos personales sensibles necesitan una legislación europea. Se ofrece una posible solución a través del nuevo instrumento jurídico de un Consorcio Europeo de Infraestructuras de Investigación (EDIC) introducido en el Programa de Política de la Década Digital (DDPP). Los EDIC tienen personalidad jurídica y se crean mediante una decisión de ejecución de la Comisión. Cuando un EDIC se convierta en responsable del tratamiento de la divulgación de datos, el acto de ejecución debe proporcionar la base jurídica basada en la misión del EDIC. Sin embargo, el marco jurídico del EDIC, tal como se define en la DDPP, plantea interrogantes con respecto a la suficiencia del acto de ejecución, un contratiempo que aún debe resolverse.

4. Ricard Martínez Martínez, Universidad de Valencia

Ricard Martínez Martínez, como activo experto en privacidad en el ámbito de la tecnología, inicia su discurso de apertura con las siguientes reflexiones tras haber escuchado a otros ponentes anteriores:

No se trata solo de la protección de datos, estamos hablando del futuro de los datos que impulsan las políticas públicas, los datos que impulsan el estado de bienestar, los datos que impulsan los servicios sanitarios, los datos que impulsan la sociedad. De acuerdo con el RGPD, los datos se dirigen a promover el ser humano, a promover el bien común, y este será nuestro enfoque. No se trata de prohibir el tratamiento de datos personales, se trata de tratar los datos en un entorno seguro con garantías legales.

Regulaciones como DGA, EDHS o DA consisten en empoderar a los ciudadanos, empoderar a los interesados, lo cual no es una tarea fácil porque: 1) los interesados no entienden las políticas de privacidad, 2) estamos hablando de servicios que son, en la práctica, monopolios, y 3) hay una situación de desequilibrio, particularmente en los servicios de internet, o en la red real de investigación en salud.

Una vez establecidas las condiciones límite, se considera de vital importancia trabajar los siguientes aspectos: consentimiento dinámico (diferente a la forma tradicional de dar consentimiento o de controlar los datos), consentimiento libre e inequívoco en el mundo digital, gestión de los riesgos reputacionales (que pueden mejorar la confianza en la sociedad), difusión de lo que estamos haciendo, hacer frente a un ecosistema en el que el consentimiento no es la base jurídica más adecuada (tenemos que recuperar la idea del bien común), trabajar desde una perspectiva de interés público (no individualista), fomentar el uso de tecnologías que mejoren la privacidad, garantizando las infraestructuras locales seguras, trazables y disponibles para garantizar que todos los nodos locales puedan trabajar juntos de forma federada, la implementación de cláusulas contractuales de gobernanza legal entre las diferentes partes interesadas involucradas en todos los niveles (incluidos los relacionados con la ética), y la mejora del personal de apoyo.

D. ESPACIOS DE DATOS A NIVEL NACIONAL EN TODA EUROPA

El cuarto panel, liderado por la Oficina del Dato Española, ha querido abordar los espacios de datos nacionales que ya se están desarrollando. Por ello, el Centro Europeo de Investigación (JRC, por sus siglas en inglés) de la Comisión Europea presentó su papel como institución de apoyo para el desarrollo de los espacios de datos y dos ejemplos de espacios de datos españoles.

1. Alberto Palomo, Secretaría de Estado de Digitalización e Inteligencia Artificial

El objetivo del panel "Espacios de datos a nivel nacional a través de Europa" fue mostrar ejemplos prácticos de espacios de datos en España, así como el contexto general de su despliegue e impacto según el análisis y recomendaciones realizadas por el Centro Común de Investigación. Moderado por Alberto Palomo (Oficina Nacional del Dato), el panel comenzó con Eimear Farrel (JRC) abordando el papel que ha desempeñado esta unidad dentro de la Comisión Europea a la hora de proporcionar perspectivas tecno-socio-económicas en torno a la compartición de datos, junto con recomendaciones no vinculantes y buenas

prácticas. También han elaborado varios recursos para los requisitos del espacio de datos, incluido un mapa de recursos y un repositorio abierto de conocimientos, que proporciona una visión holística para las partes interesadas en el espacio de datos. A continuación, Alberto compartió la visión de Gaia-X, una iniciativa de nube y datos en una posición única que ya tiene varios proyectos faro en marcha, y compartió la importancia de un marco de gobernanza multinivel adecuado en todos los proyectos, industrias, Estados miembros y a nivel de toda la UE.

Por último, Rocío Báguena y Maite Ambrós —del Ministerio de Transportes (MITMA) y del Ministerio de Agricultura (MAPA), respectivamente— presentaron una visión del papel estratégico que juegan los espacios de datos en sus unidades, así como los proyectos en desarrollo o ya operativos. Ambos ministerios están ansiosos por promover un modelo de producción sostenible para la innovación basada en datos. En resumen, estos diálogos evidenciaron que se están realizando esfuerzos hacia el despliegue efectivo de espacios de datos en diferentes sectores, por lo que las organizaciones europeas están digitalizando sus cadenas de valor gracias a datos fiables y trazables, generando así una ventaja competitiva en los mercados internacionales.

2. Eimear Farrell, Centro Común de Investigación de la CE

Eimear Farrell, como experta científica en el campo de los datos, centra su exposición en el trabajo desarrollado por el Centro Común de Investigación como centro de ciencia y conocimiento de la Comisión Europea.

Está involucrada en el desarrollo de tecnología que permita reunir tanto las políticas como la implementación de la DGA, DA, DMA, AIA y todas las regulaciones digitales. El catálogo del JRC cuenta con más de 3000 conjuntos de datos para investigación, y se han publicado más de 500 documentos relacionados con la compartición de datos.

La última publicación en la que ha colaborado activamente está relacionada con los espacios de datos: "*European Data Spaces - Scientific Insights into Data Sharing and Utilisation at Scale*".[1] Destaca el mapeo del panorama de los intermediarios que desempeñan un papel importante en la DGA y en los espacios de datos y una lista de requisitos funcionales y no funcionales de los espacios de datos, la forma en que operan y sus atributos de calidad. También señala que están trabajando en una nueva publicación sobre PETs.

También participa en el apoyo a la Comisión Europea en el diseño y despliegue del espacio de datos del Pacto Verde, donde se están probando los componentes de Gaia-x para comprobar las compatibilidades en este entorno.

[1] https://publications.jrc.ec.europa.eu/repository/handle/JRC129900

3. Rocío Báguena Rodríguez, Ministerio de Transportes de España

Rocío Báguena, como experta en tecnología y datos del transporte, habla sobre el papel del Ministerio de Transportes y Agenda Urbana en relación con los datos y la compartición de datos y lo refiere a la "Estrategia Nacional sobre la movilidad segura, sostenible y conectada 2030". La estrategia incluye un total de 8 pilares y hasta 150 medidas diferentes, y 2 de estos 8 pilares son fundamentales para los datos y la compartición de datos: el pilar 5 relacionado con la movilidad inteligente (o transporte de una persona) y el pilar 6 con las cadenas logísticas intermodales inteligentes. Incluyen varias medidas y proyectos vinculados.

También habla del punto de acceso nacional para el transporte multimodal, que recoge información de empresas privadas y públicas. Ha contribuido al sistema de datos abiertos con más de 100 conjuntos de datos que se pueden utilizar para la investigación y las estadísticas.

4. Maite Ambrós, Ministerio de Agricultura, Pesca y Alimentación

La adopción de la digitalización en el sector agroalimentario es cada vez mayor, las iniciativas de compartición de datos están muy extendidas, sin embargo, el sector aún no está familiarizado con el concepto de espacio de datos. La Política Agrícola Común se ha centrado demasiado en el seguimiento y el control de los fondos públicos y los datos para hacerlo (uso secundario), mientras que el uso primario de los datos debe reforzarse aún más, para mejorar la rentabilidad, el comportamiento medioambiental y ayudar a los productores primarios a mantener una posición más fuerte en la cadena agroalimentaria asimétrica.

Hay algunas iniciativas prometedoras que podrían convertirse en verdaderos espacios de datos, muchas de las cuales se desarrollan en torno a cooperativas de datos como intermediarios de datos que garantizan un entorno de confianza, objetivos compartidos y gobernanza inclusiva. Un ejemplo es el de la Confederación Española de Cooperativas Agroalimentarias[2] que está recogiendo los datos necesarios para solicitar las ayudas PAC, en un registro digital de explotaciones agrarias o "cuaderno de campo digital"[3] pero con la idea de mejorarlo con un sistema SIG, y comparar las prácticas agrícolas de las cooperativas entre sí. En otros ejemplos españoles, las asociaciones de ganaderos son las cooperativas de datos, que recopilan los datos en la práctica y la producción cotidiana de los ganaderos, así como de los investigadores, los árboles genealógicos sobre la filiación y los centros de inseminación artificial como el proyecto "GC4 Sheen",[4] donde se desarrollará una Plataforma de Datos Federados

[2] https://www.agro-alimentarias.coop/

[3] https://www.agro-alimentarias.coop/posts/cooperativas-agro-alimentarias-de-espana-e-hispatec-presentan-el-cuaderno-de-campo-cooperativo

[4] Hatps://gc4sheep.com/

en la Nube con Inteligencia Artificial para la Mejora Genética y Reproductiva de la Oveja Lechera Nacional.

La Acción de Coordinación y Apoyo AgriDataSpace está mapeando estas iniciativas en toda la UE y definiendo componentes comunes de espacios de datos desde múltiples ángulos (técnico/tecnológico, empresarial y organizativo/operativo) pero con la perspectiva de los agricultores, las pymes y las particularidades del sector agroalimentario[5]*.*

E. PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO TÉCNICAS EN ESPACIOS DE DATOS

Por último, el quinto panel, liderado por ENISA, pretende aportar una visión de cómo tener en cuenta la protección de datos desde el diseño y por defecto en estos escenarios de acceso masivo a datos, presentando la visión de tres expertos en protección de datos de diferentes áreas de especialización.

1. Prokopios Drogkaris, ENISA

La Ley de Gobernanza de Datos crea un marco en el que los titulares de datos, los intermediarios de datos y los usuarios de datos cooperan para garantizar la compartición, el tratamiento y el uso responsables y conformes de los datos, incluidos los datos personales. La protección de datos desde el diseño y por defecto son dos principios fundamentales para proteger los derechos y libertades de las personas y cumplir con los requisitos del RGPD.

Sin embargo, ¿es la aplicación práctica de estos principios algo completamente nuevo o podemos extraer lecciones de la experiencia que ya tenemos en las operaciones de tratamiento existentes? ¿En qué medida las normas técnicas pueden apoyarnos en ese proceso y cuáles son los elementos más específicos que debemos tener en cuenta? ¿Cuál es el estado de las medidas técnicas y organizativas que pueden dar soporte técnico a la protección de datos en los espacios de datos de la UE?

2. Isabel Barberá, Rhite

La confianza, la sinergia y la interoperabilidad son conceptos comunes en los espacios de datos. Si bien son esenciales, a menudo se centran en la construcción de sistemas eficientes y no siempre en la sinergia crítica con los usuarios, los usuarios finales y los interesados.

Para que la confianza florezca, la sensación de seguridad es primordial. Los PET y los rigurosos sistemas de calidad de datos son valiosos componentes de protección, pero por sí solos no pueden garantizar la confianza. Para establecer realmente la confianza, necesitamos transparencia. Esto solo puede lograrse reconociendo el valor de los datos y los intereses comunes de todos los

[5] https://agridataspace-csa.eu/

participantes. Este entendimiento compartido es lo que puede crear sinergia e interoperabilidad.

Explorar el panorama de amenazas de los espacios de datos genera algunas preocupaciones. Si bien los intermediarios de datos tienen el potencial de fomentar la confianza y la sinergia, ¿quién debería seleccionarlos? ¿Participantes, Estados miembros, entidades europeas en general? La incorporación de los derechos de los interesados en las arquitecturas del espacio de datos y el abordaje de las desventajas de los costes operativos para las pymes también son preocupaciones fundamentales. La interoperabilidad se basa en estándares, pero la gobernanza sigue siendo una pregunta abierta: ¿quién es responsable? ¿Quién es responsable de identificar y mitigar los riesgos?

Tal vez sea hora de añadir una "E" de "Ético" al acrónimo FAIR (Findable, Accessible, Interoperable, Reusable) para subrayar la importancia de la ética y la protección de los derechos fundamentales en el discurso de los espacios de datos.

3. Marie Charlotte Roques Bonnet, Asesor legal en protección de datos

La creación de un marco técnico y organizativo coherente que apoye la compartición eficiente de datos personales dentro de todos los sectores pertinentes de la UE (espacios comunes de datos de la UE) es esencial para que sean eficientes. Todos los titulares de datos que deseen promover la reutilización de datos personales para el bien social y económico, ya sean entidades públicas o privadas, responsables o encargados, deben demostrar responsabilidad, mediante, según corresponda, mecanismos internos renovados, acuerdos de compartición de datos y programas de gestión de privacidad sensatos (PMPs). Para ello, algunos componentes básicos de la rendición de cuentas son:

1. *Identificación clara de responsabilidades y obligaciones para los titulares y usuarios de los datos.*
2. *Gobernanza interna efectiva de la compartición de datos personales.*
3. *Gobernanza externa cooperativa de la compartición de datos personales*
4. *Adición de una sección dedicada al "Programa de compartición de datos" en los PMPs de los titulares de datos.*
5. *Diseño de herramientas específicas de rendición de cuentas de compartición de datos para reducir los riesgos (es decir, "mecanismos de altruismo de datos").*
6. *Objetivos equilibrados de seguridad y mitigación de riesgos para garantizar una calidad suficiente de los datos que se van a compartir.*
7. *Evaluación ética de las prácticas previstas de compartición de datos, tanto para los titulares como para los usuarios de los datos.*
8. *Compartición transparente de información entre los titulares y receptores de datos.*

9. *Encuadre contractual de las prácticas de compartición de datos.*
10. *Transparencia hacia las personas.*

4. Irene Kamara, Facultad de Derecho de Tilburg

Para lograr la protección de datos desde el diseño y por defecto en los espacios de datos europeos, la estandarización tiene un papel importante que desempeñar. Las normas técnicas en general fomentan la confianza entre los diferentes actores en los espacios de datos y proporcionan puntos de referencia comunes. La Ley de Gobernanza de Datos 2022/868, en su considerando 23, ya señala las normas técnicas, los códigos de conducta y la certificación como buenas prácticas.

En el ámbito de la protección de datos y la privacidad desde el diseño y por defecto, las organizaciones europeas e internacionales de estandarización han publicado varias normas que también son relevantes para los espacios de datos. En concreto, varios requisitos, controles y procesos de protección de datos existentes por diseño y por defecto son relevantes tanto para la capa de gobernanza/organizativa como para la capa técnica de los espacios de datos. Entre ellos se encuentran los requisitos de comunicación entre el consumidor y el interesado, las metodologías de evaluación de riesgos, los planes de respuesta a la violación de datos, la definición de los requisitos del sistema y la arquitectura.

Sin embargo, también existen algunos desafíos en el uso de las normas técnicas existentes. Entre ellas se encuentran, por ejemplo, que las normas técnicas actuales sobre protección de datos por diseño y por defecto se centren en las organizaciones, en lugar del ciclo de vida del tratamiento en todas las organizaciones. Además, los enfoques y técnicas específicos pertinentes para los espacios de datos, como el enfoque de computación a datos, que también se proporciona en la propuesta sobre los espacios de datos sanitarios europeos, no se reflejan en las normas de protección de datos existentes.

III. MESAS DE DEBATE

La parte final del evento se centró en una serie de mesas de trabajo en las que los asistentes debatieron sobre temas relacionados con la protección de datos en los espacios de datos.

Estas mesas estaban abiertas a la discusión, a plantear preguntas abiertas, a identificar los principales problemas, así como a proponer soluciones o, al menos, a identificar dónde se seguiría trabajando para alcanzarlos.

Cada mesa de trabajo estuvo a cargo de dos moderadores que se encargaron de presidir las discusiones, compilar un resumen de los resultados y presentar en la sesión plenaria que concluyó el evento.

Las ocho mesas de trabajo que se instalaron abordaron los siguientes temas. Cada mesa contó con una representación variada de 10 personas en promedio:

1. Actores, partes interesadas y roles

2. Gestión de riesgos y EIPD
3. Derechos de los interesados
4. Transparencia y rendición de cuentas
5. Delegado de Protección de Datos
6. Autoridades de ejecución y supervisión
7. Tecnologías para la compartición de datos
8. Brechas de datos y medidas de seguridad

A. ACTORES, PARTES INTERESADAS Y ROLES

Ricard Martínez Martínez (Universitat de València) y Jesús Rubí Navarrete (AEPD) como moderadores de la mesa de trabajo "Actores, partes interesadas y roles" llegaron a las siguientes conclusiones tras debatir con los participantes de esta mesa de trabajo.

Los temas abordados en esta mesa de trabajo ponen de manifiesto los principales retos de cualquier proyecto para definir un espacio de datos y los casos de uso en él. La identificación de los roles de cada actor en un espacio de datos es clave para establecer los mecanismos de gobernanza adecuados e identificar las responsabilidades de protección de datos, entre otros.

Con base en las experiencias actuales, no es posible definir a priori los roles desplegados en un Espacio de Datos. Esto se debe a la complejidad de su variedad de actividades y estructura. Un ejemplo rápido de consideraciones que se pueden comenzar a enumerar para definir/diseñar un espacio de datos podría ser:

A. Gestión administrativa ordinaria.
   - Gestión de usuarios del espacio de datos: registro de usuarios de acceso a datos, consulta de catálogos de conjuntos de datos o cuadros de mando de aplicaciones, suscripción a boletines informativos, etc.
   - Compromisos de Titulares de Datos o Nodos Federados: proceso de negociación para la incorporación al espacio de datos.
   - Gestión de cookies, redes sociales, canales de comunicación, eventos, difusión.
   - Gestión interna de los recursos humanos.

B. Gestión del espacio de datos en la prestación de servicios de tratamiento. En este entorno, pueden producirse todas las relaciones posibles, entre las que se incluyen:
   - Responsables sucesivos (destinatarios en una divulgación por transmisión o por una simple consulta de datos: titular de los datos a la plataforma, titular de los datos a las divulgaciones de los usuarios o compartición de datos).
   - Corresponsabilidad (gestión conjunta del espacio de datos por parte de los titulares de los datos, uso de los datos por parte de un consorcio de investigación o de los usuarios y titulares de los datos que acceden a los datos).

- Soporte para el almacenamiento o tratamiento por parte de uno de los nodos (encargados de tratamiento de datos).
- Escenarios de anonimización: soporte para el proceso de anonimización (encargado de tratamiento de datos) y la compartición y uso de datos anonimizados respaldados por acuerdos legales específicos, como acuerdos de compartición/transferencia de datos (titulares de datos) y términos y condiciones (usuarios de acceso a datos).

Por lo tanto, los Espacios de Datos deben tener necesariamente un modelo de definición de roles basado en las Directrices 07/2020 del EDPB sobre los conceptos de responsable y encargado del tratamiento en el RGPD.

Debe considerarse la posibilidad de que una sola persona física (física o jurídica) asuma múltiples funciones que puedan influir en los procesos de toma de decisiones. Por lo tanto, la definición de roles debe incluir procesos de gobernanza para declarar y resolver cualquier conflicto de intereses.

Como se ha destacado en las consideraciones anteriores, los modelos de espacio de datos, en particular los entornos federados, definen relaciones de alta complejidad. Además, estos modelos pueden evolucionar y sufrir cambios por diversos motivos. Por ejemplo, una federación de espacios de datos compuesta por un consorcio de socios puede transformarse en una entidad jurídica independiente. La incorporación de nuevos titulares de datos o la introducción de nuevos servicios de tratamiento también pueden afectar a los roles desplegados en un espacio de datos.

Por otra parte, la creación de órganos o entidades por diferentes reglamentos no implica necesariamente una definición clara de sus funciones. Por ejemplo, si una región con administración propia crea un espacio de datos para la explotación de su información con fines primarios o secundarios, opera como responsable. Si también ofrece servicios de tramitación a municipios dentro de su territorio, podría actuar como encargado del tratamiento. Sin embargo, si el propósito es implementar el análisis de datos para el diseño de políticas territoriales, podría haber sucesivos responsables o corresponsables. Por otro lado, en una infraestructura abierta a todas las partes interesadas, la definición de la finalidad del uso secundario recae en el usuario que accede a los datos.

A menos que se trate de casos muy claramente definidos, el legislador carece de información suficiente para la definición de roles. Además, si el diseño es defectuoso, debería dar lugar a la no aplicación de la ley cuando contradiga el RGPD. En este contexto, debe evitarse el riesgo de conflictos institucionales o disputas jurídicas. En consecuencia, no es aconsejable definir roles a priori por ley.

En resumen, se identifican las siguientes afirmaciones como clave a tener en cuenta a la hora de definir/diseñar un espacio de datos:

- El diseño legal del espacio de datos debe contemplar, asumir e implementar el modelo de gobernanza que surge del RGPD.

- Cada espacio de datos debe implementar procedimientos para una determinación clara de los roles del RGPD y regir los posibles conflictos de intereses.
- La predeterminación legal de los roles podría ser un riesgo. La corresponsabilidad debe considerarse especialmente arriesgada debido a la dificultad de su aplicación.

Algunas reflexiones adicionales a considerar serían:

- Los usuarios de datos, el espacio de datos y los titulares de datos deben ser especialmente responsables en la definición de la base legal para el tratamiento y la aplicación de los procedimientos de cumplimiento del RGPD. En particular, la cooperación y la transparencia entre todos los agentes en actividades como la evaluación de impacto de la protección de datos o la evaluación de impacto de los riesgos de la inteligencia artificial deben ser extremadamente pertinentes.
- Los Espacios de Datos deben proporcionar una información institucional clara sobre sus procedimientos y modelo de gobernanza. La política de gobernanza debe basarse en pruebas reales.
- Los miembros del grupo de trabajo consideran que no existen condiciones adecuadas de madurez para cumplir con el RGPD en los espacios de datos europeos.
- Los facilitadores, el personal técnico son esenciales. Los organismos públicos y los futuros servicios de intermediación deben tener en cuenta sus funciones, perfiles y puestos de trabajo, como la inversión obligatoria. El grupo de trabajo subraya que no hay suficientes recursos humanos y cultura interna del sector público y privado sobre el cumplimiento del RGPD para proporcionar certidumbre, seguridad y confianza a la sociedad. Este esfuerzo será especialmente relevante para las actividades de altruismo de datos.

B. GESTIÓN DE RIESGOS Y EIPD

Isabel Barberá (Rhite) y Rafael Pastor Vargas (UNED) como moderadores de la mesa de trabajo "Gestión de riesgos y EIPD" llegaron a las siguientes conclusiones tras debatir con los participantes de esta mesa de trabajo.

Estas preguntas abiertas propuestas que impulsaron el debate en la mesa de trabajo fueron: ¿Cómo detectar y gestionar los riesgos creados a partir de la puesta en común de los datos (por ejemplo, posibilidades de vinculación))? ¿Quién es responsable de mitigar esos riesgos? ¿Existen metodologías para evaluar los riesgos de reidentificación asociados con el proceso de compartición de datos, teniendo en cuenta los posibles tipos de datos? ¿Qué tipos de escenarios de riesgo son comunes en los espacios de datos? ¿Cómo deben evaluarse y gestionarse? ¿Se pueden dar recomendaciones generales para la EIPD o son específicas para cada espacio de datos según el sector y el tipo de datos procesados? ¿Pueden los métodos cuantitativos de evaluación de riesgos ayudar a mejorar los resultados de la EIPD?

Los miembros de la mesa de trabajo consideraron que existe una relación compleja entre los roles asociados a la gestión/uso de los datos. Además, cuanto mayor sea la complejidad del tratamiento de datos, mayor será el riesgo de que los datos se vean comprometidos. Para mitigar estas complejidades, se necesita orientación específica para hacer frente a las EIPD. Tener un entorno complejo requiere EIPD específicas (por rol/usuario, por dominio de datos) y la EIPD global del entorno/ecosistema de espacio de datos en particular.

También se consideraron cuestiones como quién debería estar a cargo de la evaluación de riesgos dentro de un ecosistema de espacio de datos. Podría ser el supervisor, el intermediario de datos o incluso el encargado de tratamiento de datos, por lo que, de nuevo, parece necesario contar con un sistema de rendición de cuentas descentralizado de evaluación de riesgos. Es necesario distinguir qué entidad es responsable de la ejecución y supervisión de la evaluación de riesgos, en función de la estructura del espacio de datos implementado. La estandarización de las EIPD es otro tema importante, y se considera prioritario contar con puntos específicos que pregunten/expliquen aspectos del análisis de riesgos en los escenarios de compartición masivo de acceso a datos en un espacio de datos, que no existen en la actualidad. A esto se suman las consideraciones sobre la influencia de los derechos fundamentales en las evaluaciones de impacto (FRIA, Evaluación de Impacto sobre los Derechos Fundamentales). Esto aumentaría la calidad y la confianza, pero también requiere más concienciación, educación, formación y recursos.

Otro tema crítico a considerar son los riesgos de la reidentificación en entornos de datos, donde es posible no conocer con precisión la riqueza semántica del entorno y tener la posibilidad de tener información que permita esta reidentificación. Debe tenerse en cuenta durante el proceso de diseño. Más adelante, podría probarse con herramientas automatizadas para facilitar la eficiencia y la productividad en el espacio de datos. Además, al ser un entorno vivo con constantes actualizaciones de datos, es recomendable utilizar evaluaciones dinámicas y no tradicionales basadas solo en periodos de tiempo. Una vez más, la automatización es imprescindible.

A modo de resumen de las aportaciones se puede concluir que es necesario seguir las siguientes líneas para el futuro:

- La orientación para hacer frente a las EIPD y su normalización es necesaria y prioritaria.
- Incluir las consideraciones de la FRIA (Evaluación de Impacto sobre los Derechos Fundamentales) en la evaluación de riesgos.
- Proporcionar (tener) una biblioteca de amenazas específicas para los espacios de datos, modelando relaciones complejas entre los roles de los espacios de datos.
- Centrarse en la evaluación relacionada con la reidentificación como parte obligatoria de la EIPD.
- Los espacios de datos complejos necesitan diferentes EIPD, por lo que es esencial definir una jerarquía de EIPD y una definición clara de las

responsabilidades en la evaluación de riesgos (dinámica) en los espacios de datos.

C. DERECHOS DE LOS INTERESADOS

Marie Charlotte Roques Bonnet (experta en Derecho de la Privacidad de la UE) y Javier Gómez Prieto (ENISA) como moderadores de la mesa de trabajo "Derechos de los interesados" llegaron a las siguientes conclusiones tras debatir con los participantes de esta mesa de trabajo.

En los espacios de datos, más que nunca, el control de los usuarios sobre sus datos determinará la eficacia de sus derechos como interesados. Por lo tanto, es esencial que sepan cuándo sus datos personales: i) se procesan para otros fines, ii) se procesan en un formato anonimizado o identificable. Sobre la base de este mapeo inicial, las personas estarán facultadas para: 1/ compartir sus expectativas razonables (véanse los considerandos 47 y 50 del RGPD), 2/ ejercer sus derechos en la práctica, como el derecho a consentir o retirar fácilmente el consentimiento (es decir, en unos pocos clics).

El grupo reconoció que el manejo irracional de los derechos por parte de los interesados sería un problema, pero admitió que deberíamos poder ejercer nuestros derechos fácilmente. En este sentido, es fundamental lograr un equilibrio entre el suministro de datos personales y la obtención de un servicio (enfoque basado en el riesgo y enfoque basado en el impacto). Se proporcionará una información proactiva y accesible de forma digerible: construir un consentimiento válido de forma tangible: explicando cómo podrían ejercer los derechos y evitar modelos engañosos / actividades ocultas. El grupo señaló que la investigación pública (por ejemplo, la actividad no rentable para las empresas) será uno de los principales objetivos de los espacios de datos.

En caso de que los datos personales se procesen en un formato directamente identificable, se deben tomar las medidas técnicas y organizativas (MTO) adecuadas, y las obligaciones siguen siendo tan exigentes como en el RGPD. El ejemplo del impacto de las brechas de seguridad, que podría ser mayor en los espacios de datos interoperables, planteó la cuestión de un derecho que podría ser específico de los espacios de datos y que consistiría en el ejercicio de un derecho a que sus datos personales se omitan o nunca se introduzcan. Otro ejemplo fue el de la descentralización técnica, que es inherente a los espacios de datos: el almacenamiento debe dividirse para dividir y minimizar los riesgos.

Todos los participantes coincidieron en la contribución decisiva de las buenas prácticas de ciberseguridad y valoraron las buenas prácticas de los espacios de datos claros (es decir, claves de descifrado almacenadas por organismos públicos, autorización de acceso, riesgos específicos de interoperabilidad, privacidad diferencial). Todos los participantes se mostraron a favor de una fuerte seudonimización por defecto. Se evaluó que la anonimización probablemente "no funcionaría": sería posible identificar e inferir que se trata de datos inútiles porque no son lo suficientemente cualitativos como para ayudar a la investigación y al tratamiento innovador de datos.

Parte del debate también abordó puntos de vista específicos relacionados con la «Ley del espacio de datos sanitarios de la UE». Una de las primeras observaciones fue que disponer de demasiados instrumentos legislativos no facilitaría, por su naturaleza y por definición, la interoperabilidad de espacios de datos tan diferentes, algo que a priori va en contra del buen ejercicio de los derechos de los interesados, y no solo de la portabilidad (artículo 20 del RGPD). Esos derechos deben enmarcarse en la práctica, comenzando con una evaluación sobre el terreno y una fase de consulta multisectorial de abajo hacia arriba. Los elementos clave de estas intersecciones se abordarían precisamente a través de las nociones de: a) "formato estructurado, de uso común y legible por máquina", y b) cuando sea técnicamente viable". Esta tormenta de ideas y el cribado operativo podrían impulsarse mediante grupos de trabajo específicos de la UE e internacionales o mediante la revisión de la evaluación comparativa de buenas prácticas sectoriales.

Por último, deben tenerse en cuenta las limitaciones contextuales y operativas en todos los niveles de toma de decisiones. En este frente, la principal conclusión de las discusiones podría resumirse de la siguiente manera: no es un problema, las prácticas serían diferentes de un sector a otro, y los MOT se manejarían de manera diferente, pero es esencial que las reglas y principios sean un estándar abierto fácilmente replicable de un sector a otro, de un espacio de datos a otro. Este enfoque determinará si las personas están facultadas en la práctica para ejercer sus derechos de manera simple y coherente. En pocas palabras, los marcos legislativos para los entornos y los espacios de datos favorables a la tecnología no deben especificar los derechos de los interesados en un enfoque sectorial, sino simplemente crear herramientas coherentes, de un sector a otro, para permitirles simplemente ejercer dichos derechos.

D. TRANSPARENCIA AND RESPONSABILIDAD PROACTIVA

Javier Huerta Bravo (Cullen International) y Andrés Calvo Medina (AEPD) como moderadores de la mesa de trabajo "Transparencia y Rendición de Cuentas" llegaron a las siguientes conclusiones tras debatir con los participantes de esta mesa de trabajo.

Los participantes coincidieron en que los espacios de datos son bastante incipientes, en las primeras etapas de desarrollo. Por lo tanto, en esta etapa es difícil enmarcar todas las obligaciones de rendición de cuentas y transparencia en un contexto de espacio de datos.

Los participantes también señalaron que, cuando proceda, los requisitos de rendición de cuentas y transparencia en virtud del Reglamento General de Protección de Datos (RGPD) de la UE podrían tener que complementarse con las obligaciones de rendición de cuentas y transparencia establecidas en otra legislación digital pertinente, incluido el proyecto de Ley de Inteligencia Artificial de la UE. También se abordó la creciente complejidad del marco normativo de la UE en materia de datos.

Las discusiones giraron en torno al concepto de rendición de cuentas y cómo este principio fundamental relacionado con el tratamiento de datos personales en el RGPD debe entenderse en el contexto de los espacios de datos como una parte inherente de

los mismos por diseño, y algunos de los intervinientes en los espacios de datos deben requerir asistencia, como debería ser el caso de las startups y las pymes.

Uno de los participantes señaló que la rendición de cuentas significa "volver a cada operación de tratamiento de datos y poder explicar lo que estaba sucediendo en un momento dado", para demostrar el cumplimiento. Sin embargo, los participantes destacaron que la rendición de cuentas es diferente del cumplimiento, ya que es un aspecto importante de este último.

La definición anterior hace especial hincapié en la dimensión de trazabilidad del principio de rendición de cuentas. Ser capaz de rastrear las operaciones de tratamiento de datos se vuelve más relevante en el contexto de los espacios de datos, ya que se espera que involucren muchas operaciones de tratamiento de datos, responsables y encargado de tratamiento de datos, y sujetos de datos.

Además, los participantes señalaron que no debería haber un modelo fijo o rígido de rendición de cuentas para los espacios de datos. En cambio, la rendición de cuentas (o los modelos de rendición de cuentas aplicables) debe ser dinámica, basada en las tecnologías más avanzadas y lo suficientemente flexible como para adaptarse a las especificidades de cada espacio de datos y de cada tratamiento de datos personales.

Se podrían implementar diferentes tecnologías de mejora de la privacidad (PETs) y soluciones técnicas adaptadas a las características de cada espacio de datos. La proactividad implícita en el principio de rendición de cuentas se vuelve crucial en este contexto.

Además, los participantes señalaron que, dado que la línea entre los datos personales y los no personales suele ser bastante difusa, las normas de rendición de cuentas del RGPD deben aplicarse tanto a los datos personales como a los no personales.

Los participantes también abordaron formas efectivas de garantizar la transparencia en los espacios de datos. Estuvieron de acuerdo en que los procesos de transparencia podrían ser automatizados o semiautomatizados, y que los investigadores y la academia podrían ayudar a las organizaciones en este aspecto.

Además, los participantes debatieron sobre la forma en que las normas, las especificaciones, la certificación y las etiquetas comunes podrían ayudar a aportar transparencia a los espacios de datos. La propuesta de la Comisión Europea para un espacio de datos sanitarios ya señala algunos de estos instrumentos y puede servir de base para otros espacios de datos.

E. DELEGADO DE PROTECCIÓN DE DATOS

Anna Lytra (CEPD) y Carlos Saiz (ISMS Forum.) como moderadores de la mesa de trabajo "Delegado de Protección de Datos" llegaron a las siguientes conclusiones tras debatir con los participantes de esta mesa de trabajo.

Varios DPOs que participaron en esta mesa redonda expresaron que enfrentan dificultades para identificar el papel de los diferentes actores involucrados en los espacios de datos como responsables/encargados/subencargados. Esto puede tener un

impacto en la calidad del asesoramiento del DPD a su responsable/encargado dentro de la organización sobre varios asuntos.

La ley española de protección de datos no prevé multas para la administración pública en caso de infracción. Teniendo esto en cuenta, los DPO pueden enfrentarse a algunas dificultades sobre cómo promover/fomentar el cumplimiento dentro de su organización.

Los DPO participantes expresaron que sería muy apreciada una red de la UE en la que los DPD puedan intercambiar sus prácticas y los retos a los que se enfrentan en el contexto de los espacios de datos.

F. AUTORIDADES DE EJECUCIÓN Y SUPERVISIÓN

Enrique Factor Santoveña (AEPD) y Manuel González Seco (CTPD) como moderadores de la mesa de trabajo "Autoridades de Ejecución y Supervisión" llegaron a las siguientes conclusiones tras debatir con los participantes de esta mesa de trabajo.

Los principales temas tratados en esta mesa de trabajo fueron: la gobernanza, la posición de las diferentes y muchas autoridades, la innovación en los espacios de datos y la necesidad de entregar valor.

La gobernanza se ha abordado planteando la siguiente pregunta: "¿Debería la gobernanza incluir una aplicación estricta o un enfoque suave? Después de una discusión entre los participantes, se llegó a las siguientes conclusiones:

- El enfoque suave ha funcionado mejor, con un sistema de bonus/malus basado en la reputación. Pero debe haber una aplicación estricta.
- Importancia de la colaboración público-privada, para aplicar directrices que sean exigibles y eficaces.
- Necesidad de extender las medidas de ejecución estrictas a las partes interesadas públicas: medidas significativas (no financieras), como la prohibición del tratamiento, que puedan aplicarse en la protección de datos, que podrían tener un efecto importante.
- También hay que tener en cuenta a las pymes.

Pasando al segundo tema debatido, relacionado con la posición de diferentes y numerosas Administraciones, los participantes concluyeron que:

- La coordinación es necesaria y puede ser difícil cuando se trata de reguladores independientes.
- Superposición de esferas de competencia. Interacción entre diferentes marcos regulatorios a diferentes niveles.
- Coordinación entre reguladores: no solo debe coordinar, sino también impulsar la colaboración y el uso de los datos para los fines correctos. Puede darse el caso de recibir, por ejemplo, nueve requisitos de diferentes autoridades y a diferentes niveles (regional, nacional, europeo).
- Reforzar la adquisición de talento: lecciones aprendidas de la ciberseguridad que se pueden aplicar en este ámbito.

Pasando al siguiente tema "innovación en los espacios de datos", todos los participantes coincidieron en afirmar que la regulación no es un freno; establece un entorno de trabajo que garantiza el desarrollo respetando los derechos fundamentales. El marco nacional no debe ser un elemento disuasorio para la implementación de espacios de datos.

Y, por último, a la hora de debatir sobre la necesidad de entregar valor, la mesa de trabajo concluyó que los espacios de datos solo funcionarán si aportan valor. Estos nuevos entornos requieren una gran inversión y un costoso mantenimiento. El valor añadido no tiene por qué ser económico, el objetivo final es beneficiar a todos los participantes.

G. TECNOLOGÍAS PARA LA COMPARTICIÓN DE DATOS

Christina Michelakaki (FPF) y Miguel Peñalba Moldes (AEPD) como moderadores de la mesa de trabajo "Tecnologías para la compartición de datos" llegaron a las siguientes conclusiones tras debatir con los participantes de esta mesa de trabajo.

La mesa de trabajo arrojó luz sobre cuestiones críticas e identificó conclusiones perspicaces. Una pregunta central que surgió fue si existen tecnologías capaces de garantizar el cumplimiento del RGPD al compartir datos. Surgieron dos perspectivas distintas: la de la industria y la de las entidades proveedoras de herramientas y medios técnicos y la de los reguladores. Desde el punto de vista de la industria, se discutió que las empresas dudan en compartir datos utilizando PET u otras tecnologías debido a la falta de conocimiento sobre estas soluciones y debido a la falta de orientación regulatoria sobre el tema. Muchos participantes destacaron el hecho de que los "casos de éxito" en la compartición de datos no se demuestran lo suficiente, lo que hace que las empresas no estén dispuestas a confiar en las nuevas tecnologías. Desde el punto de vista regulatorio, se dejó en claro que los reguladores no están en condiciones de indicar qué tecnología funciona para la compartición de datos, dado que una medida que puede ser apropiada para un determinado contexto podría ser ineficaz para otro.

Otro bloque de cuestiones que surgieron durante el taller se refería a los factores técnicos que van en contra de la compartición de datos en el contexto específico de un espacio de datos. En primer lugar, se hizo un llamamiento para que se elaboraran instrumentos y normas que garantizaran la rendición de cuentas y la confianza en los procesos de compartición de datos. Además, los participantes señalaron la falta de soluciones técnicas europeas, observando que no hay muchos competidores en el espacio de la UE. También se abordó la cuestión de la calidad de los datos. Entonces, la madurez de los datos se consideró una preocupación secundaria en comparación con la cuestión crítica de la interoperabilidad. Los problemas surgieron al intentar utilizar soluciones proporcionadas por diferentes proveedores de PET debido a la falta de interoperabilidad. Por lo tanto, se propuso la elaboración de normas como medio para infundir confianza entre todas las partes implicadas en la compartición de datos.

A continuación, el taller exploró ejemplos concretos e historias de éxito en la compartición de datos y las herramientas utilizadas para este fin. En el contexto de los

servicios de salud, se destacó el cifrado en los sistemas basados en la nube como una solución que permite realizar cálculos directamente sobre datos cifrados sin necesidad de descifrarlos. Sin embargo, la gran cantidad de datos y la complejidad de las cláusulas contractuales plantean retos considerables. También se demostró que las empresas prefieren el enfoque de una compartición centralizada de datos en el que una empresa instrumental obtiene el consentimiento de los clientes. Sin embargo, se acordó que este escenario conlleva riesgos inherentes, como la retirada del consentimiento. Por lo tanto, se sugirió que un cambio hacia el aprendizaje federado, en el que la computación se lleva a los datos en lugar de trasladarlos a una ubicación centralizada, podría mitigar esos riesgos. Más concretamente, el aprendizaje federado permite el entrenamiento de modelos en orígenes de datos distribuidos sin compartir los datos sin procesar. Esta herramienta puede ser utilizada por las empresas para trabajar de forma colaborativa sin compartir realmente ideas, pero también obteniendo ventajas. No obstante, persistieron las preocupaciones sobre la competencia y los posibles monopolios, lo que puso de manifiesto la necesidad de considerar posibles soluciones no solo desde la perspectiva del cumplimiento del RGPD, sino también desde el punto de vista del derecho de la competencia.

Para concluir, los participantes compartieron sus ideas sobre los desafíos, las oportunidades y las consideraciones en torno a la compartición de datos y las tecnologías. Hicieron hincapié en la importancia de la concienciación, el desarrollo de normas y la necesidad de herramientas versátiles como el aprendizaje federado para superar los desafíos y permitir una compartición de datos seguro y eficiente en el futuro.

H. BRECHAS DE DATOS Y MEDIDAS DE SEGURIDAD

Olga Rierola Forcada (APDCAT) e Irene Kamara (Tilburg Law School) como moderadoras de la mesa de trabajo "Brechas de datos y medidas de seguridad" llegaron a las siguientes conclusiones tras debatir con los participantes de esta mesa de trabajo.

El alto volumen de datos personales y no personales procesados en los Espacios de Datos y la interconexión permanente entre diferentes sistemas de compartición e compartición de datos, aumentan el riesgo de que ocurran brechas de datos personales (o aumentan el riesgo/probabilidad de materialización de brechas de datos personales). Los participantes de la mesa redonda discutieron las principales preocupaciones, riesgos y vulnerabilidades en relación con las brechas de datos en los espacios de datos y las buenas prácticas.

Los moderadores presentaron un escenario ficticio de un espacio de datos de salud en el que los hospitales públicos y privados compartirían los registros de salud de los pacientes con fines de investigación. De acuerdo con este escenario, los hospitales comparten los datos personales sensibles de manera vulnerable desde el punto de vista de la seguridad.

Los participantes identificaron varios riesgos y debilidades, derivados de una perspectiva de gobernanza, pero también debido a la alta complejidad (complejidad

organizativa, legal y tecnológica) del tratamiento de datos en los espacios de datos, lo que los convierte en objetivos atractivos para los atacantes.

Incluso cuando se implementan fuertes medidas de seguridad, pueden surgir brechas masivas de datos personales en los espacios de datos, con un alto impacto en los derechos y libertades de los interesados, y también posiblemente un alto impacto a nivel social.

La escala es una fuente importante de riesgo para las brechas de datos en los espacios de datos (múltiples actores, cantidad de datos), pero también en arquitecturas complejas y modelos de espacios de datos, donde los datos se compartirán entre espacios de datos o en diferentes capas dentro del mismo espacio de datos. Se prevén nuevos tipos de ataques. Además, los participantes destacaron el riesgo de ataques por parte de adversarios no pertenecientes a la UE, pero también de legislación extranjera que podría permitir a las autoridades extranjeras solicitar el acceso a los datos compartidos en el espacio de datos, por ejemplo, con fines policiales (por ejemplo, la Ley CLOUD de EE. UU.). Este podría ser el caso cuando la implementación de servicios que almacenan datos personales en países no pertenecientes a la UE (como las transferencias internacionales de datos) pueda presentar riesgos para los derechos y libertades de los interesados.

Pueden producirse otros riesgos en el proceso de hacer que el conjunto de datos sea interoperable para un espacio de datos determinado.

La distribución de la responsabilidad entre los diferentes actores en los espacios de datos es incierta. Las diferentes arquitecturas y los diferentes modelos de gobernanza, en combinación con la multitud de actores con diferentes derechos y roles, serán problemáticos en el caso de una infracción, por ejemplo, causada por un ataque malicioso. En tal caso, no habrá propiedad del problema y, por lo tanto, no se implementarán los procedimientos y medidas apropiados para informar y mitigar el impacto de la violación de datos, al menos de manera adecuada.

La clasificación jurídica de los actores como responsables del tratamiento, corresponsables del tratamiento, encargados del tratamiento o subencargados del tratamiento dependerá de cómo se establezca la gobernanza y la infraestructura del espacio de datos.

Otra cuestión debatida fue la aplicabilidad de diferentes marcos jurídicos en paralelo (diferentes requisitos de notificación de incidentes). Además de la notificación y comunicación de brechas de datos personales en virtud del RGPD, y de forma independiente de ellas, los responsables del tratamiento también deben ser conscientes de cualquier obligación de notificar incidentes de seguridad en virtud de otra legislación asociada que pueda aplicarles y si esto también puede exigirles que notifiquen a la autoridad de control una brechas de datos personales al mismo tiempo.

Ese será el caso de la Ley de Resiliencia Operativa Digital (DORA) para el sector financiero, o la Directiva NIS2 que obliga a los operadores de servicios esenciales y a los proveedores de servicios digitales a notificar los incidentes de seguridad a su autoridad

competente. Esto significa que, cuando dichos incidentes sean o se conviertan en brechas de datos personales en virtud del RGPD (y no siempre es así, ya que hay incidentes de seguridad que no comprometen los datos personales, y viceversa), dichos operadores y proveedores estarían obligados a notificar a la autoridad supervisora de protección de datos por separado de los requisitos de notificación de incidentes de la NIS2 y otros marcos legales aplicables. Esas obligaciones de información siguen diferentes plazos, requieren la presentación de informes a diferentes competentes, como se ha visto, y el tipo de información que debe notificarse también difiere.

Un aspecto clave es la asignación clara de roles y responsabilidades antes de que se establezca el espacio de datos y pueda tener lugar cualquier brecha de datos. En el caso de una brecha de datos personales, los procedimientos y responsabilidades deben estar claros de antemano, esto podría hacerse con los Términos y Condiciones del espacio de datos, acuerdos contractuales entre los diferentes actores, acuerdos de licencia, gestión de acceso basada en roles y obligaciones de diligencia debida.

A continuación, es crucial contar con un marco de gestión de riesgos. El marco debe incluir un plan de procedencia de los datos, planes de respuesta a emergencias, pero también los actores deben participar en diferentes escenarios de brechas de datos.

Otra recomendación se refiere a la automatización de los procesos que, en la medida de lo posible, debe detectar las infracciones. Además, se recomienda un uso proactivo de las técnicas de mejora de la privacidad.

Incluso con los mejores estándares de ciberseguridad y medidas de seguridad, las brechas de datos personales seguirán ocurriendo, por lo que las PET (tecnologías de mejora de la privacidad) también serán relevantes en los espacios de datos. El término "compartición" se entenderá como "acceso y tratamiento", que no es lo mismo que transferencia y copia de datos personales.

La información y la comunicación a los interesados es importante. Las formas dinámicas de presentar información sobre los riesgos para sus derechos y libertades pueden ser una buena práctica.

El uso de mecanismos ampliamente aceptados, como normas técnicas, certificación y códigos de conducta para demostrar el cumplimiento, será útil para los espacios de datos. Debemos basarnos en lo que ya existe y explorar dónde hay lagunas.

Es necesaria la formación y concienciación sobre los riesgos de ciberseguridad y privacidad, antes de que los titulares, intermediarios y usuarios accedan a los espacios de datos. Una buena práctica sería una plataforma de transferencia de conocimientos para los actores del espacio de datos.

Por último, las filtraciones de datos y el cumplimiento deben tratarse como un problema de la cadena de suministro. El hecho de que un actor disponga de todas las medidas técnicas y organizativas necesarias no significa que no herede las vulnerabilidades o debilidades de otro actor, por ejemplo, un titular de datos que proporcionó un conjunto de datos o un intermediario que seleccionó un conjunto de datos. En tal escenario, se debe evitar que la responsabilidad se diluya entre las

organizaciones involucradas en el tratamiento, las cuales deben actuar de manera coordinada en la gestión de riesgos para los derechos y libertades de los interesados.

IV. CONCLUSIONES FINALES

Los participantes en las mesas de trabajo compartieron sus puntos de vista, inquietudes e ideas respecto a los Espacios de Datos y la protección de datos personales. Al intentar resumir las discusiones, se evidenció que aún quedan varias preguntas abiertas, principalmente por la novedad del concepto, pero también por las diferentes posibilidades de tratamiento de datos personales y los diferentes actores involucrados.

El principal elemento común de las discusiones fue que necesitamos evaluar la experiencia y los conocimientos de la aplicación de los principios del RGPD a las operaciones de tratamiento existentes e intentar, por analogía, transferirlos a las operaciones de tratamiento en espacios de datos. Puede que esto no sea tan sencillo al principio, pero nos permitirá tener en cuenta todas las buenas prácticas y procesos existentes.

Otro elemento común de los debates fue la necesidad de consulta y orientación a nivel nacional y europeo. Espacio de Datos es un nuevo concepto que aún está en desarrollo mientras exploramos todo su potencial. Durante estas primeras fases de despliegue, las partes interesadas deben poder compartir sus experiencias, prácticas y soluciones identificadas, así como consultar a los reguladores.

El último elemento que se destacó fue la evolución del panorama tecnológico para la compartición de datos. A medida que evolucionan las nuevas tecnologías, como el aprendizaje federado, debemos ser capaces de identificar y evaluar tanto los riesgos como las oportunidades para cumplir con los principios del RGPD. En ese sentido, los análisis y las buenas prácticas serían apreciados, pero también beneficiosos.

V. REFERENCIAS

Evento AEPD-ENISA “Espacios de datos en la Unión Europea: Sinergias entre protección de datos y espacios de datos, los retos de la UE y las experiencias españolas"[oct 2023]

AEPD - ENISA conference on Data Spaces